



QUALYS SECURITY CONFERENCE 2019

Threat Hunting with Qualys: Going Beyond Your EDR Solutions

Chris Carlson
VP Strategy, Qualys, Inc.

Adversary Threat Tactics are Changing

Early 2010s

Zero-day Vulnerabilities

(Nation State, Industrial Espionage, Black Market)

Today

Rapidly weaponizing newly-disclosed vulnerabilities

(Good, Fast, Cheap – Pick 3)

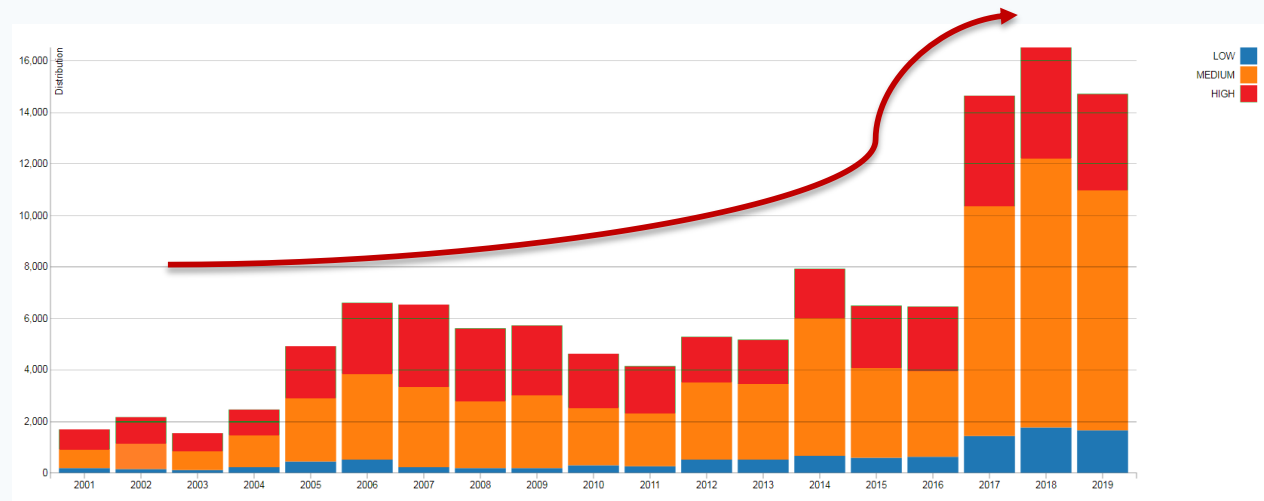
Known Critical Vulnerabilities are Increasing

14-16K vulnerabilities are disclosed 2017-2019

30-40% are ranked as “High” or “Critical” severity

Worm-able Vulnerabilities are increasing (WannaCry, BlueKeep)

“Mean Time to Weaponize” is rapidly decreasing year/year



Let's Talk About BlueKeep

(RDP Vulnerability)

U.S. Govt Achieves BlueKeep Remote Code Execution, Issues Alert

By [Sergiu Gatlan](#)

 June 17, 2019  11:13 AM  1

US company selling weaponized BlueKeep exploit

An exploit for a vulnerability that Microsoft feared it may trigger the next WannaCry is now being sold commercially.



By [Catalin Cimpanu](#) for Zero Day | July 25, 2019 -- 09:06 GMT (02:06 PDT) | Topic: Security

7/30/2019
12:00 PM



Robert
Lemos

BlueKeep Exploits Appear as Security Firms Continue to Worry About Cyberattack

The lack of an attack has puzzled some security experts, but the general advice remains that companies should patch their vulnerable systems more quickly.

Just Two Weeks Ago

EDITOR'S PICK | 380,176 views | Nov 3, 2019, 04:43am

Windows 'BlueKeep' Attack That U.S. Government Warned About Is Happening Right Now



Davey Winder Senior Contributor

[Cybersecurity](#)

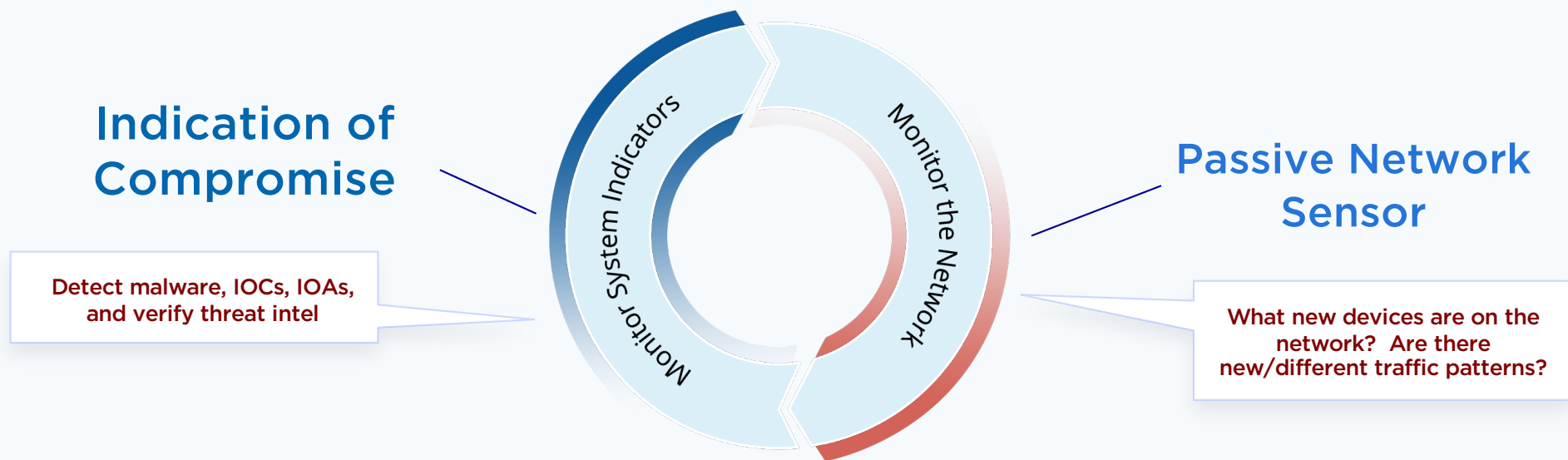
I report and analyse breaking cybersecurity and privacy stories



Get Proactive – Reduce the Attack Surface

- AI** **VM** Immediately discover assets and vulnerabilities
- PM** Notify IT asset owner to patch / stop the instance
- PC** **SCA** Change configuration to limit unauthorized access
- CSA** Control network access / cloud security groups
- IOC** Add endpoint detection and response

Proactively Hunt, Detect, and Respond



Qualys IOC – Hunt Using Threat Intel

NotPetya Ransomware spreading using ETERNALBLUE Vulnerability and Credential Stealing October 6, 2017

On June 27, 2017, NCCIC [13] was notified of Petya malware events occurring in multiple countries and affecting multiple sectors. This variant of the Petya malware—referred to as NotPetya—encrypts files with extensions from a hard-coded list.

Additionally, if the malware gains administrator rights, it encrypts the master boot record (MBR), making the infected Windows computers unusable. NotPetya differs from previous Petya malware primarily in its propagation methods using the ETERNALBLUE vulnerability and credential stealing via a modified version of Mimikatz.

Technical Details

Anti-Virus Coverage

VirusTotal reports 0/66 anti-virus vendors have signatures for the credential stealer as of the date of this report

Files

Delivery – MD5: 71b6a493388e7d0b40c83ce903bc6b04

Installation – MD5: 7e37ab34ecdcc3e77e24522ddf4852d

Credential Stealer (new) – MD5: d926e76030f19f1f7ef0b3cd1a4e80f9

Secondary Actions

NotPetya leverages multiple propagation methods to spread within an infected network. According to malware analysis, NotPetya attempts the lateral movement techniques below:

2 Search for the file hash here...

The screenshot shows the Qualys Enterprise Hunting interface. At the top, there's a navigation bar with 'DASHBOARD', 'HUNTING', 'INCIDENTS', and 'ASSETS'. The 'HUNTING' tab is active. Below the navigation bar, there's a 'Hunting' section with a large blue box containing the number '2' and 'Total Events'. To the right of this box is a search bar with the hash 'd926e76030f19f1f7ef0b3cd1a4e80f9' and a dropdown menu set to 'Last 7 Days'. Below the search bar is a timeline chart showing events from October 4th to 12th. A table below the chart shows related FIM events. The table has columns for 'TIME', 'OBJECT', 'ASSET', and 'SCORE'. Two events are listed, both for 'svvchost.exe' on assets 'WIN2008R2-11566' and 'WIN7-320860-T44'.

TIME	OBJECT	ASSET	SCORE
a day ago 3:58:48 PM	svvchost.exe C:\14279270823	WIN2008R2-11566 10.11.114.113	
a day ago 12:22:57 PM	svvchost.exe C:\793972740527	WIN7-320860-T44 10.11.114.109	

1 Threat intelligence lists attack information ...

3 Find the object there.

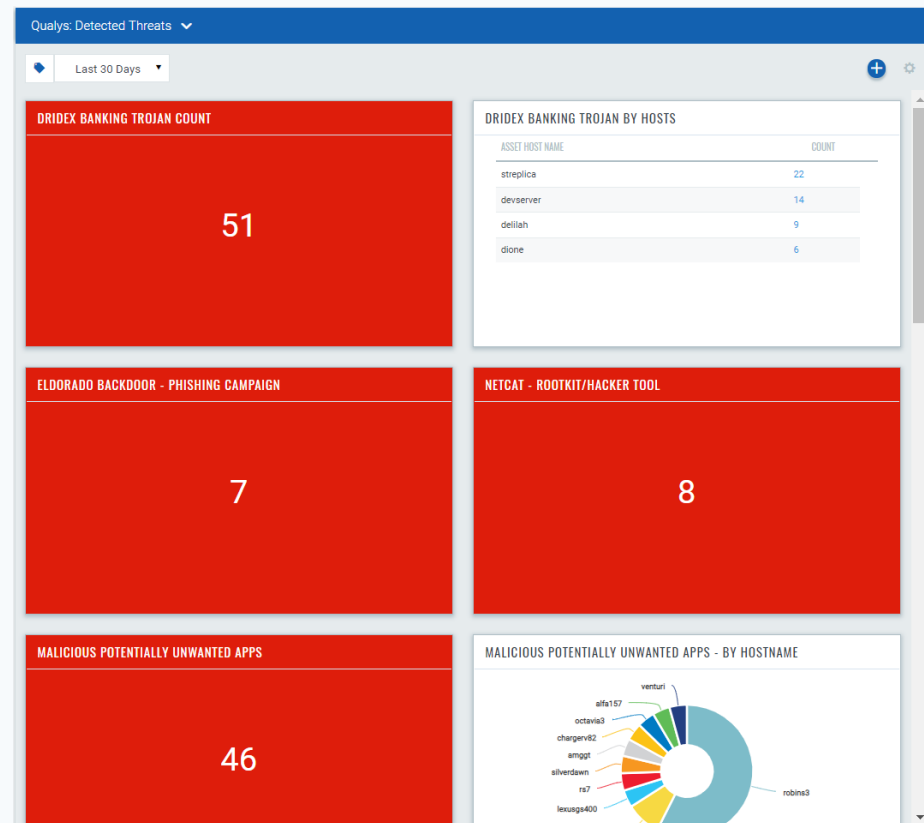
Detect Malware Missed by Anti-Virus

UK Government Contractor

- “Big 4” anti-virus installed
- Qualys Agent for Vulnerability Mgmt
- Added Qualys IOC on existing agents
- 256 hosts

Qualys IOC discovered...

- Dridex Banking Trojan (51)
- 4 domain controllers infected
- Backdoors (7) installed due to phishing campaigns
- Netcat (8) root kits installed
- 46 PUAs installed



Demo

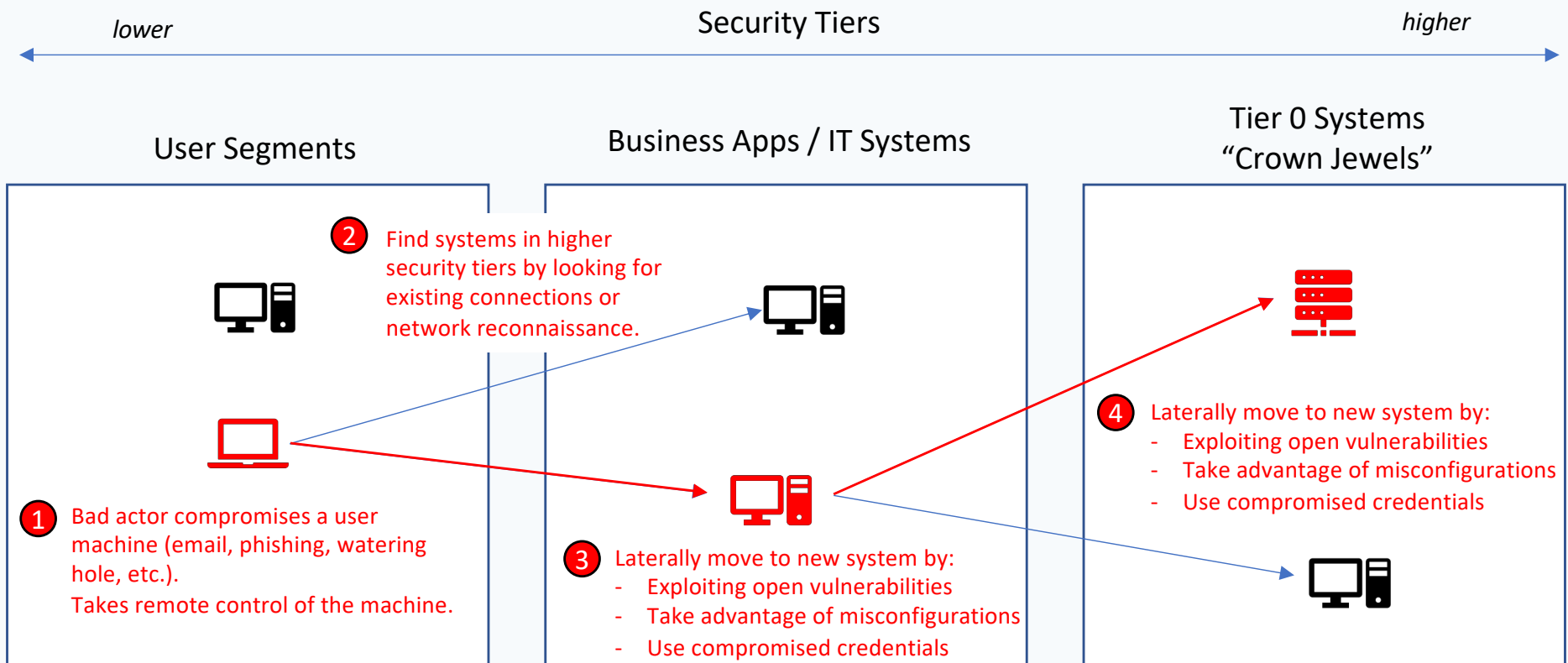
9aa730979342f8d719e730f1a2081d8e9852da646ce2fbd9ce5e5301de25a5c5

Beyond Endpoint Detection and Response: How can I better protect my crown jewels?

Threat Hunting Assumptions:

- Every user machine can be compromised – it only takes one
- Every Remote Code Execution (RCE) vulnerability can be exploited
- Local Privilege Escalation and Credential Harvesting to move laterally
- System misconfigurations are often overlooked and easy to exploit
- Network segmentation is rarely used internally due to management
- All attacks are not equal: can Adversaries reach my Critical Servers?

Adversary Lateral Movements (Attack Paths)



Finding Attack Paths

Network Reachability

Determine connections between hosts using Cloud Agent 

Passive + Active network collection

Store these connections in a Graph Database for fast query

+

Asset Security Posture

Remote Code Execution Vulnerabilities  

System Misconfigurations  

Malware and Indicators of Activity 

**Attack Path Discovery
to
Prioritize Patching and
Improve Security Defenses**

Network

Topology

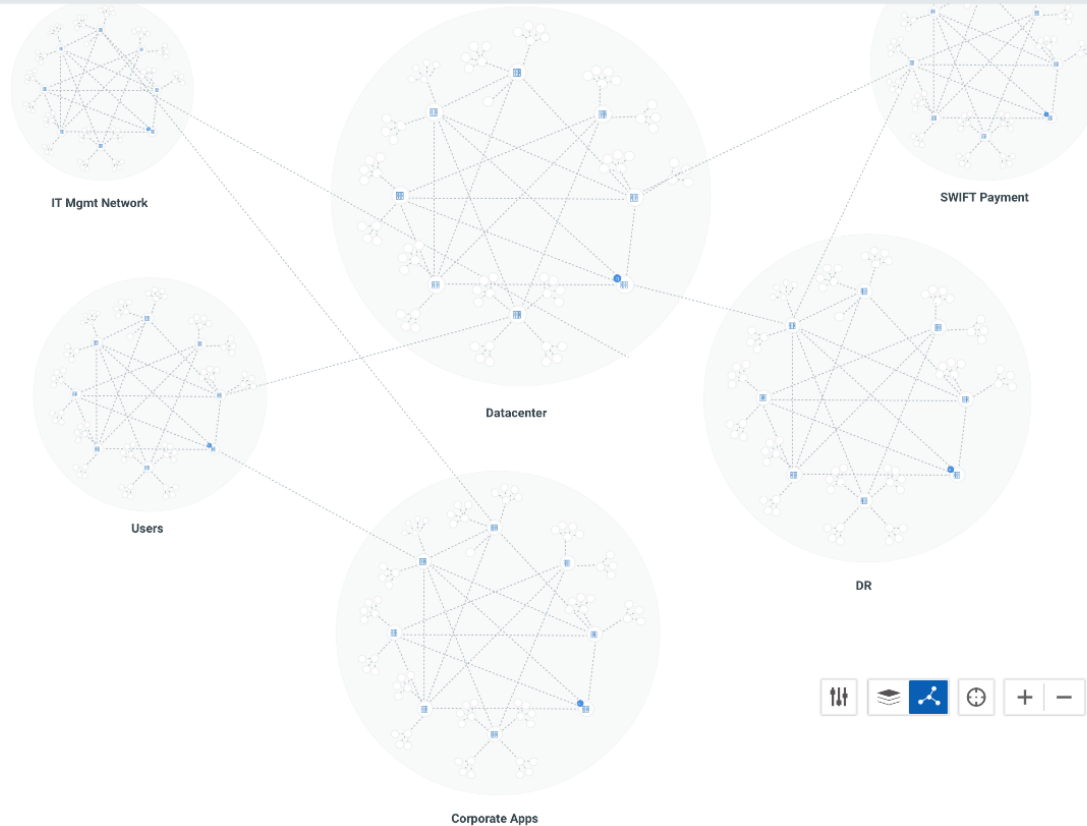
List View

🔍 Search

Last 7 days



Group Assets by...



Network

Topology

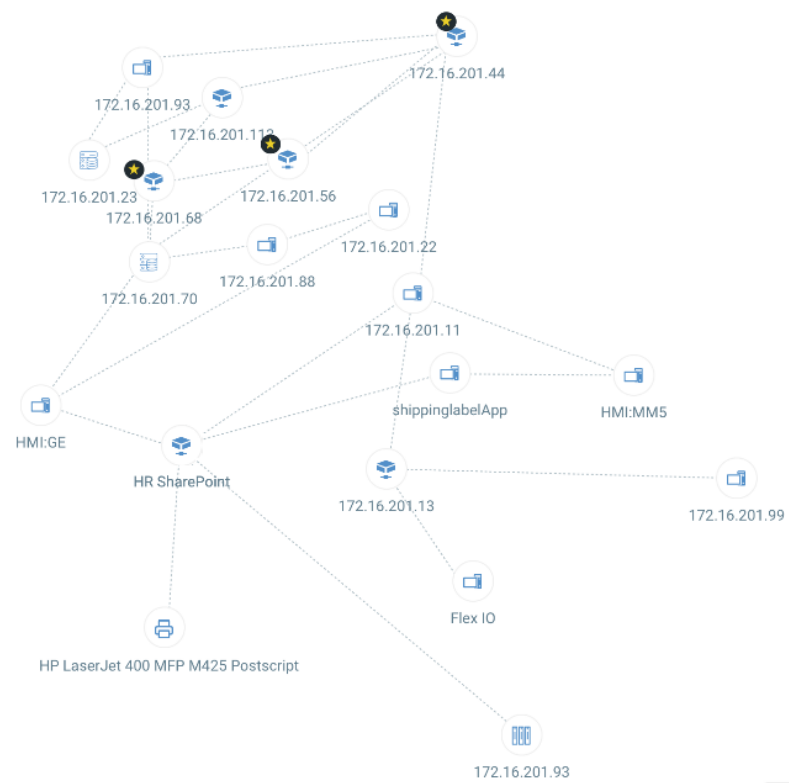
List View

Search

Last 7 days



Group Assets by...



Network

Topology

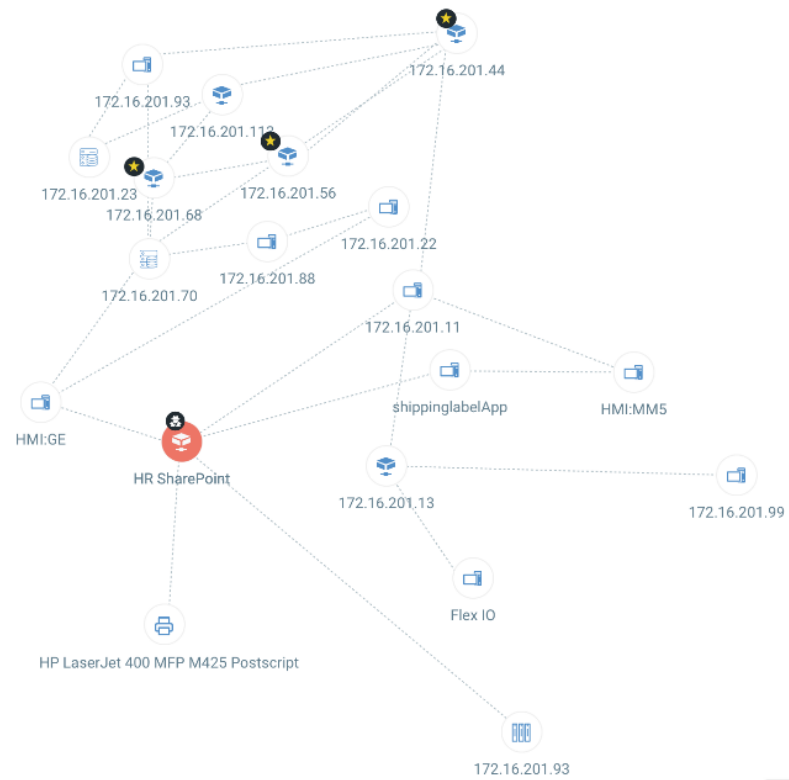
List View

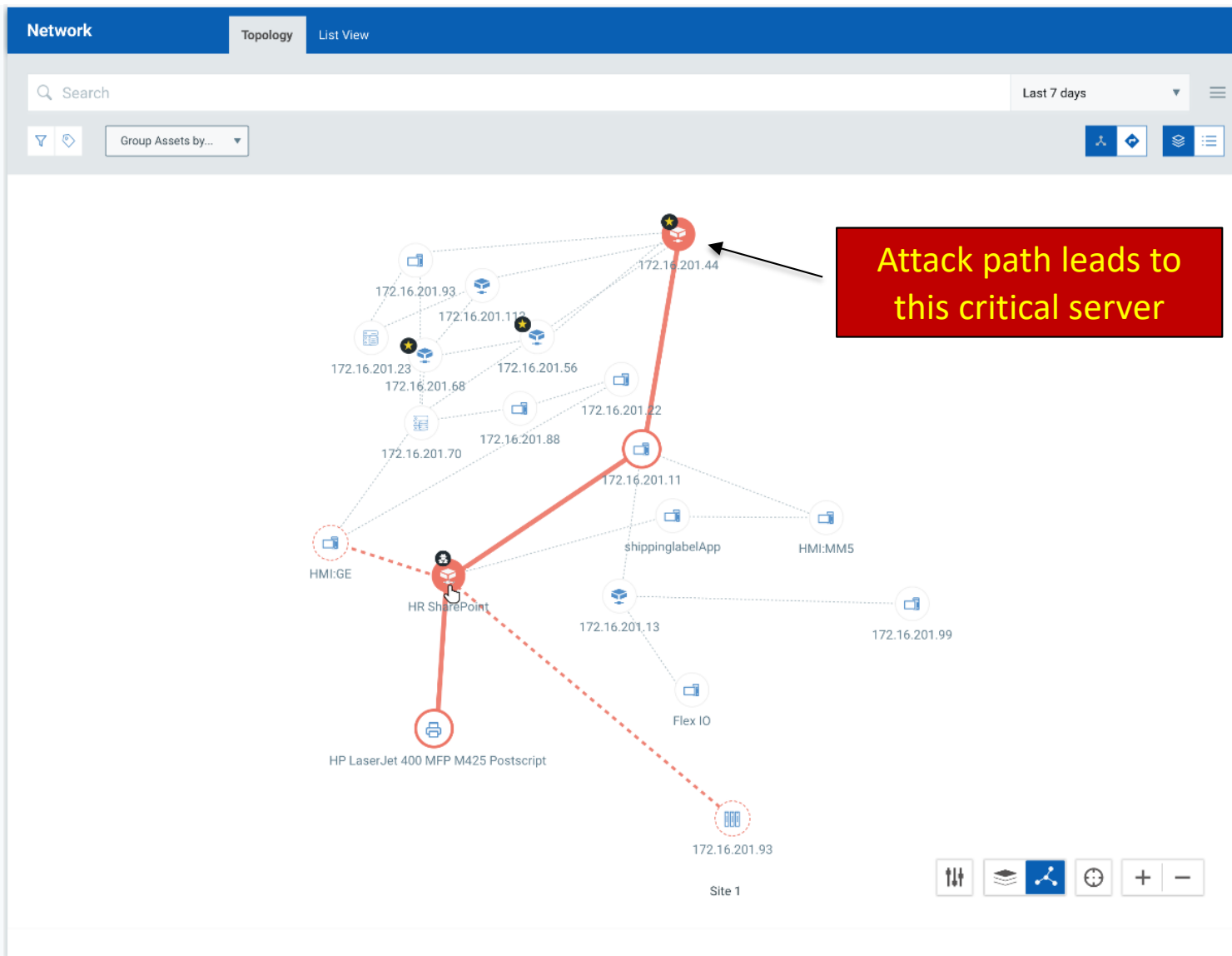
Search

Last 7 days



Group Assets by...







Attack Path Discovery for Proactive Threat Hunting and Response Priority

Hunting

675K

Total Events

TYPE

file	258K
mutex	9.84K
network	19.4K
process	3.99K
registry	384K

EVENT ACTION

created	642K
established	4.65K
listening	14.7K
running	13.8K

SCORE

10	14
9	38
8	191
6	4
5	121

🔍 1 more

✕ 5ceec909f3dfc890fdd1e76d6f3cc093465c9d980d68b9987fc3f5eb289b6bd2

Active View ▾



1 - 50 of 675335



TIME ▾		OBJECT		ASSET	SCORE	DETAILS
3 minutes ago 8:35:03 PM	⚙	WindowsAzureTelemetryService.exe C:\WindowsAzure\GuestAgent_2.7.41491.949_2019-1...	🪟	WIN10PMIOC4 13.64.103.58,10.1.1.10	—	
3 minutes ago 8:35:03 PM	⚙	QualysAgent.exe C:\Program Files\Qualys\QualysAgent\QualysAgent.exe	🪟	WIN10PMIOC4 13.64.103.58,10.1.1.10	—	
3 minutes ago 8:35:03 PM	⚙	WmiPrvSE.exe C:\Windows\System32\wbem\WmiPrvSE.exe	🪟	WIN10PMIOC4 13.64.103.58,10.1.1.10	0	
3 minutes ago 8:34:56 PM	🔗	125.227.22.242 (125-227-22-242.HINET-IP.hi... TCP CONNECTION - ESTABLISHED by svchost.exe	🪟	EC2AMAZ-Q1M5FIB 172.31.0.13,13.233.83.82	0	
3 minutes ago 8:34:56 PM	🔗	13.82.189.202 : 63733 TCP CONNECTION - ESTABLISHED by svchost.exe	🪟	EC2AMAZ-Q1M5FIB 172.31.0.13,13.233.83.82	0	
3 minutes ago 8:34:56 PM	🔗	fe80::281b:10bb:53e0:fff2%7 : 546 UDP CONNECTION - LISTENING by svchost.exe	🪟	EC2AMAZ-Q1M5FIB 172.31.0.13,13.233.83.82	0	
3 minutes ago 8:34:49 PM	🔗	64.39.104.103 (qagpublic.qg2.apps.qualys.co... TCP CONNECTION - ESTABLISHED by QualysAgent.exe	🪟	WIN10PMIOC4 13.64.103.58,10.1.1.10	—	
3 minutes ago 8:34:44 PM	🔗	211.247.115.130 : 57533 TCP CONNECTION - ESTABLISHED by svchost.exe	🪟	WIN10PMIOC4 13.64.103.58,10.1.1.10	0	
3 minutes ago 8:34:41 PM	🔗	185.209.0.22 : 36585 TCP CONNECTION - ESTABLISHED by svchost.exe	🪟	WIN10PMIOC4 13.64.103.58,10.1.1.10	0	

Hunting

5

Total Events

TYPE

file	2
mutex	1
network	1
process	1

EVENT ACTION

created	2
established	1
running	2

SCORE

10	1
9	2
8	2

✕ 5ceec909f3dfc890fdd1e76d6f3cc093465c9d980d68b9987fc3f5eb289b6bd2

Active View ▾



1 - 5 of 5



TIME ▾		OBJECT		ASSET	SCORE	DETAILS
21 hours ago 12:58:21 AM	🔗	66.85.173.57 (tar.theoutlan.com) : 443 TCP CONNECTION - ESTABLISHED by temp0291.exe	🏠	SHAREPT003 172.31.0.111	10	Trickbot Trojan
a day ago 8:19:31 PM	📄	temp0291.exe c:\Users\qualys\AppData\Roaming	🏠	SHAREPT003 172.31.0.111	8	Trickbot Trojan
a day ago 3:12:28 PM	⚙	temp0291.exe C:\Users\qualys\AppData\Roaming\temp0291.exe	🏠	SHAREPT003 172.31.0.111	9	Trickbot Trojan
a day ago 3:02:08 PM	🔒	\BaseNamedObjects\4C3D653494D1128 temp0291.exe	🏠	SHAREPT003 172.31.0.111	9	Trickbot Trojan
2 days ago 11:18:23 AM	📄	temp0291.exe c:\Users\qualys\AppData\Roaming	🏠	SHAREPT003 172.31.0.111	8	Trickbot Trojan

Network

Topology

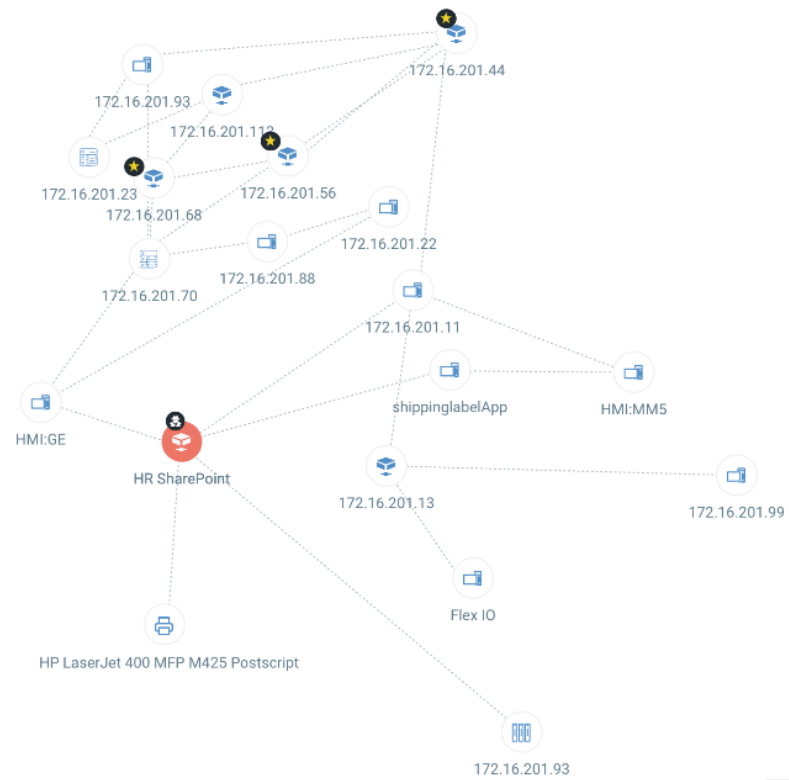
List View

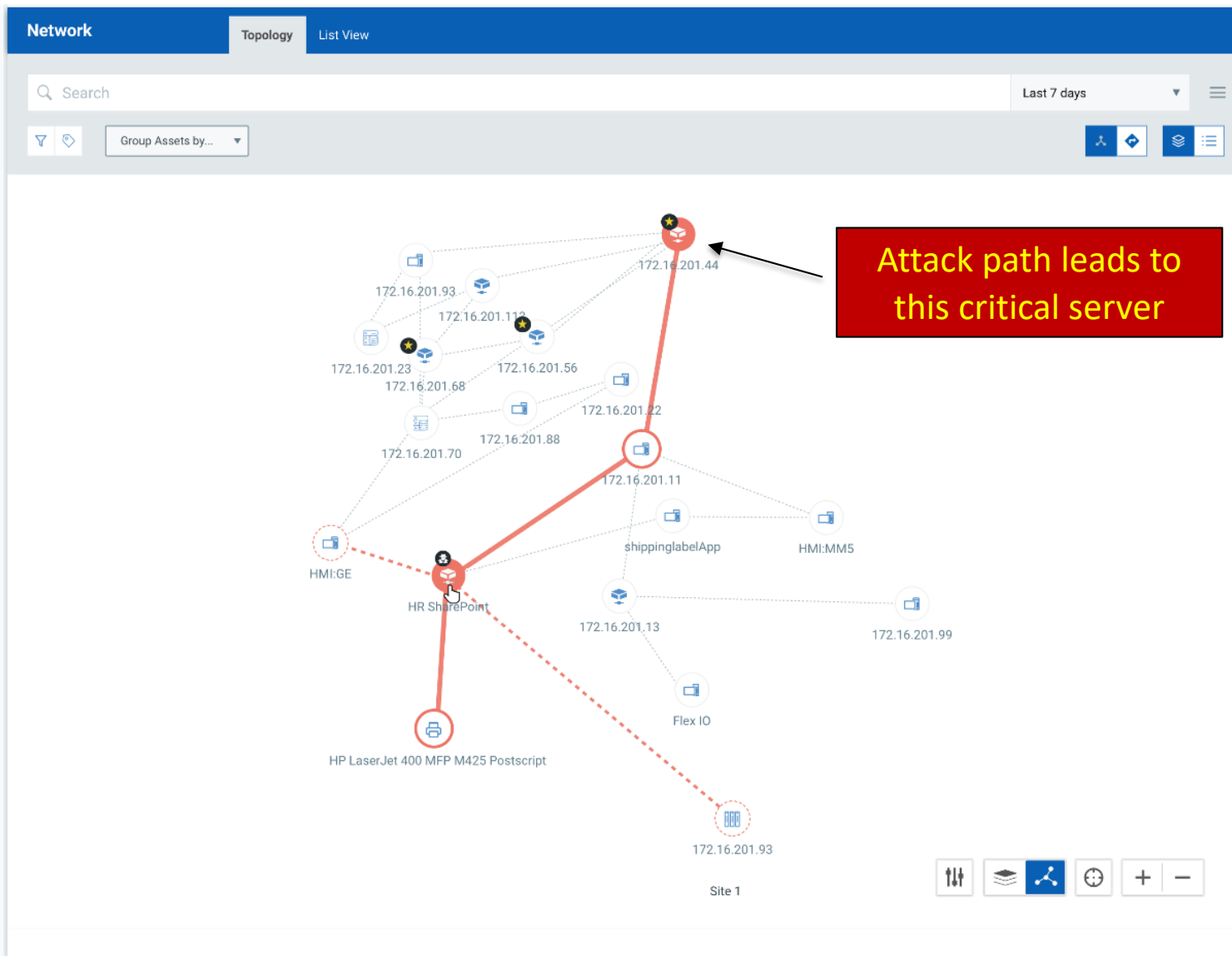
Search

Last 7 days



Group Assets by...





Network

TopologyList View

Search

Group Assets by...

HP LaserJet 400 MFP M425 Postscript

HR SharePoint

172.16.201.11

172.16.201.44

172.16.201.93

172.16.201.11

172.16.201.23

172.16.201.68

172.16.201.56

172.16.201.22

172.16.201.88

172.16.201.70

172.16.201.13

HMI:GE

HMI:MM

shippinglabelApp

Flex IO

Site 1

Actions

SharePoint

HR SHAREPOINT

172.31.0.111

New York, NY

Tags

New YorkCorporate AppsHR Apps

Share Point60_day_lastscan

INFECTIONS (4 Events)

Process: temp0294.exe

Malware: Trickbot | Risk Score: 9

File: WormDll64

Malware: Trickbot | Risk Score: 8

File: NetworkDll64

Malware: Trickbot | Risk Score: 8

File: ShareDll64

Malware: Trickbot | Risk Score: 8

Quickly investigate the host to see the active attack



Network

Search



Group As

Execute a Response

The following response will be executed for the selected processes and files on the defined hosts.

Process (1)

RISK SCORE	PROCESS NAME	MALWARE	PID	HOST
9	temp0291.exe	TrickBot	4417	SHAREPT003

☒ Kill Process☒ Quarantine File

File Type (3)

RISK SCORE	FILE NAME	MALWARE	HOST
8	WormDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003
8	NetworkDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003
8	ShareDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003

☒ Quarantine File

Cancel

Confirm

172.16.201.93

Site 1



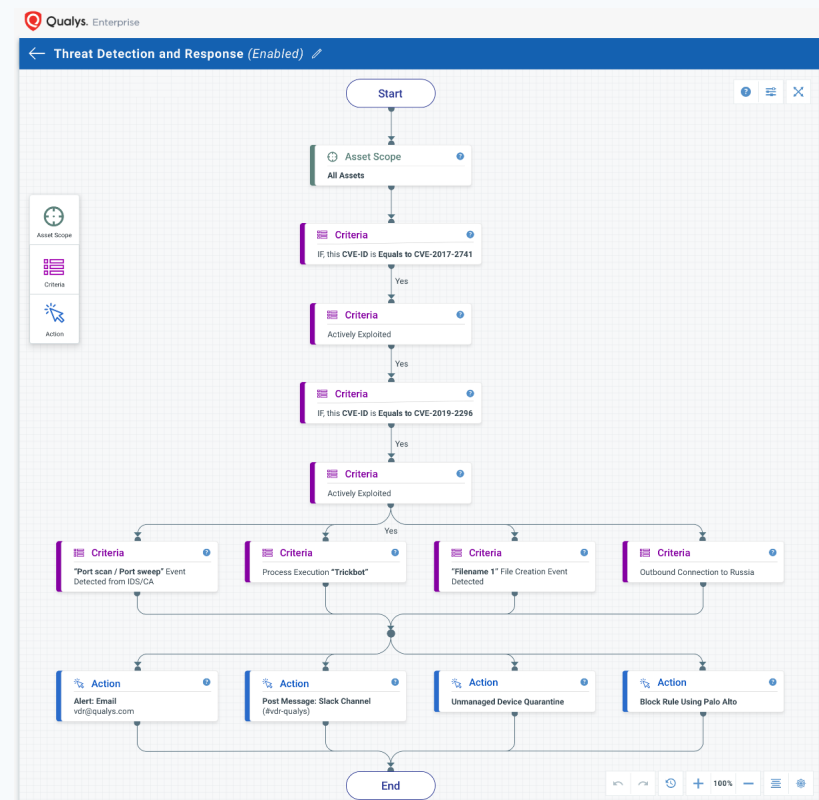
Scale Human Response with Automation

Find active attacks on endpoint using Indication of Compromise

Go beyond endpoint detection with Security Analytics – correlate user, network, application, cloud, container

Use attack path discovery as metadata to detect active attacks reaching critical assets

Automate response to protect critical assets using response playbooks





QUALYS SECURITY CONFERENCE 2019

Thank You

Chris Carlson
ccarlson@qualys.com